AMENDMENTS TO THE DRAWINGS

The attached sheet of drawings includes changes to Fig. 13. This sheet, which includes Fig. 13, replaces the original sheet including Fig. 13.

REMARKS/ARGUMENTS

Claims 1-10 stand rejected in the outstanding Official Action. Claims 1-3, 5-8 and 10 have been amended and therefore claims 1-10 remain in this application.

The Examiner's acknowledgment of Applicants' claim for priority and receipt of the certified copies of the priority documents is very much appreciated. Additionally, the Examiner's acknowledgment of consideration of the prior art listed in Applicants' previously filed Information Disclosure Statement is appreciated.

The Examiner's withdrawal of the Notice of Noncompliant Amendment is very much appreciated.

The Patent Office objects to the arrangement of the specification. It is also appreciated that the Examiner has brought the arrangement of the specification to the applicant's attention. It is noted that the objection to the arrangement appears to be an indication that the originally filed specification and drawings (transmitted from WIPO) do not meet the formality requirements of the U.S. Patent and Trademark Office. The Patent Office is reminded that the U.S. Patent and Trademark Office must comply with all articles of the Patent Cooperation Treaty (PCT) including Article 27. It has been held that:

"if the rule and interpretation of the PTO conflicts with the PCT, it runs afoul of Article 27 of the PCT which provides in part:

> (1) No national law shall require compliance with requirements relating to the form or contents of the international application different from or additional to those which are provided for in this Treaty and the Regulations." Caterpillar Tractor v. Commissioner, 231 USPQ 590, 591 (EDVA 1986).

The Patent Office has referenced this decision in the Official Gazette dated September 9, 1986 (1070 TMOG 5).

As a consequence, the Patent Office (including the Chief Draftsman's Office) may not require specification format changes as long as the originally submitted documents comply with the PCT requirements. Inasmuch as this specification was forwarded for WIPO, by definition, it meets the PCT requirements (it is not forwarded until it meets PCT requirements.). Therefore, the objection to the specification is respectfully traversed and reconsideration thereof is respectfully requested.

Notwithstanding the above, applicant has added headings and subheadings to the specification.

In section 4 of the outstanding Official Action, the specification is objected to because of the noted informalities. Applicants have amended the specification to correct the informalities noted, i.e., the deletion of the "open parenthesis" on page 11 and changing Figure 13 to read "Figure 12" on page 13, line 25.

The Examiner notes that several reference characters shown in the drawings are not mentioned in the specification. Applicants have added the reference to step 144 which is included in Figure 14 on page 14, line 31, thereby obviating this objection. Applicants have amended the label 28 in Figure 13 to read "128" as suggested by the Examiner. A replacement sheet of drawings with this correction is attached hereto. In view of the above, all objections to the drawings have been obviated and notice of PTO acceptance of the drawings is respectfully requested.

In section 6 of the Official Action, claim 10 is objected to, with the Examiner suggesting that in line 1, "dummy" be changed to read "trash." Applicant has amended claim 10 as suggested.

Claims 1, 2, 5-7 and 10 stand rejected under 35 USC §102 as being anticipated by Qiu (U.S. Patent 6,804,782). The Examiner's contention that Qiu teaches anything beyond a recognition of the problem is respectfully traversed.

The problem (solved in Qiu and in the claimed invention) is to increase the security of data processing systems so as to defeat attempts to analyze processing activity based upon power consumption. There is a characteristic power consumption signature associated with a write to a data processing register. Accordingly, information concerning the data processing being performed in association with such a write can be externally observed and hence information about whether or not such a write did or did not occur can be obtained.

Specifically, for a conditional-write data processing operation, observation of the data processing systems' power consumption may yield information about whether or not the conditional write occurred. The Qiu reference solves the problem by **masking** the power signature by producing more activity within the power signature, thereby masking any changes as a result of a conditional write data processing operation.

Thus, Qiu is just concerned with generating more activity in the power signature of a data processing system so as to defeat a power analysis attack upon its security. Qiu does not attempt to avoid the instruction being executed having a characteristic power consumption in itself and instead merely masks the power signature.

The presently claimed invention recognizes that a conditional-write instruction generates significantly different power signatures depending upon whether they do or do not result in a state changing write. The present invention solves the problem, not by masking the power signature as done in Qiu, but rather, by modifying the behavior of conditional-write program instructions so as to write to one of a data processing register desired or a trash register. Thus, there is little difference in power consumption between a conditional write instruction which does write to a data processing register or one which writes to a trash register.

In sum, where Qiu attempts to improve security by masking power variations, the present invention serves to reduce power variations between different instructions -- two very different approaches to solving the same problem of defeating a power analysis attack upon data processor security.

Applicants' independent claim 1 quite clearly specifies the requirement of a "trash register" as well as the requirement that a result data value is written to the trash register instead of to a data processing register when the condition codes within a conditional write data processing instruction do not permit a write to effect a change in state of the processor core. Thus, the last paragraph of claim 1 clearly defines the distinction between the presently claimed invention and the Qiu reference.

It is believed that the Examiner has misapprehended certain teachings in the Qiu reference in comparing alleged corresponding structures and method steps between independent claims 1 and 6 and the Qiu reference. There are three main reasons for this belief that the Examiner has misapprehended Qiu and the features of claims 1 and 6.

Firstly, claim 1 specifies a "conditional-write data processing instruction encoding condition codes." The hyphenation between "conditional" and "write" has been added to indicate that the writing is conditional, rather than the instruction itself. Suggesting that the Qiu reference teaches similar structure, the Examiner references column 4, lines 23-32 and 61-63, as well as column 5, lines 22-32. However, these sections discuss a cryptographic key determining whether a multiplication operation should be performed or not.

Quite clearly, if the Examiner is equating the "multiplication operation" of Qiu with the "data processing operation" of claims 1 and 6, then Qiu's multiplication operation would have to somehow also encode the condition codes. It is clear that cryptographic private key in Qiu which determines the condition execution of the multiplication operation does not encode condition codes, and therefore, Qiu cannot be said to disclose the claimed "a conditional-write data processing instruction **encoding condition codes**." (emphasis added).

Secondly, claims 1 and 6 recite that the condition codes specify "conditions under which said conditional-write data processing instruction will or will not be permited to write data to effect a change in the state of said processor core." The Examiner on page 5 of the Official Action points to portions of Qiu and alleges that "the cryptographic key determines the conditions under which the multiplication operation is emulated or not." However, even if this were true, this is not considered to be the equivalent of the recited portions of claims 1 and 6. In fact, Qiu discusses a cryptography private key determining whether or not a multiplication operation should be carried out.

The presently claimed invention discloses an instruction encoding condition codes which determine whether or not that instruction will or will not be permitted to write data to effect a

change in the state of the processor core, when that instruction is executed. Clearly, the cited portion of Qiu and the quoted portion of Applicants' independent claims 1 and 6 are not equivalent.

Thirdly, as mentioned above, the last paragraph of claim 1 relating to "a trash register" where the result data value is written depends upon "condition codes within said conditional-write data processing instruction." It is also noted that this writing takes place upon execution of the conditional-write data processing instruction.

Thus, in accordance with Applicants' claim, the conditional-write data processing instruction is executed and then, dependent upon the condition codes encoded therein, the result data value is either written to a trash register or to a data processing register.

The Examiner is believed to be suggesting that column 4, lines 28-35 of Qiu contains a similar disclosure. However, dependent upon a bit value in the binary key (i.e., the cryptography private key), the unnecessary mathematical operation is either performed or not. When the operation is performed in Qiu "to further emulate the implementation of the algorithm," a subsequent unnecessary store of data to memory is performed. This is not the equivalent to the feature disclosed in the "trash register" portion of claims 1 and 6. Qiu's teaching that the decision is to carry out a mathematical operation or not is not the same thing as the claimed invention of deciding to send a result data value to one of a trash register or the data processing register. Qiu's all or nothing does not disclose or render obvious performing the claimed provision of a choice between two options.

In view of the above, the Qiu reference fails to contain any disclosure of Applicants' third and fourth elements set out in claim 1 or the two method steps set out in claim 6. Should the

Examiner believe otherwise, he is respectfully requested to identify where the Qiu reference teaches each of these claimed structures and method steps. Absent any disclosure, claims 1, 2, 5-7 and 10 are clearly not anticipated under 35 USC §102 by Qiu and any further rejection thereunder is respectfully traversed.

Claims 3, 4, 8 and 9 stand rejected under 35 USC §103 as unpatentable over Qiu in view of Kissell (U.S. Patent 6,625,737). Inasmuch as claims 3, 4, 8 and 9 all depend from independent claims 1 and 6, respectively, the above comments distinguishing claims 1 and 6 from the Qiu reference are herein incorporated by reference.

There is no suggestion that the Kissell reference teaches any of the three features noted above in claims 1 and 6 which are missing from the Qiu reference. Thus, even if combined, Qiu and Kissell do not disclose the subject matter of claims 1 and 6, let alone the claims dependent thereon.

Additionally, the Examiner has failed to provide any "reason" or "motivation" for combining the Qiu and Kissell references. Finally, since Qiu's teaching of performing the mathematical operation or not performing it is dramatically different from the claimed invention of deciding which among two registers a result data value will be stored is so different as to lead one of ordinary skill in the art away from the structure and method of Applicants' claims 1 and 6, respectively. The fact that Qiu teaches away from the claimed invention is further evidence of the non-obviousness of independent claims 1 and 6 and all claims dependent thereon.

Having responded to all objections and rejections set forth in the outstanding Official Action, it is submitted that claims 1-10 are in condition for allowance and notice to that effect is respectfully solicited. In the event the Examiner is of the opinion that a brief telephone or

personal interview will facilitate allowance of one or more of the above claims, he is respectfully requested to contact Applicants' undersigned representative.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____

Stanley C. Spooner
Reg. No. 27,393

SCS:kmm
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100